VACANCY NOTICE FOR TEMPORARY AGENT SELECTION

Job title (same as on the job description)	**Team Leader – Principal Operations Officer**
Reference	**CLIMA/COM/2026/526348**
Application deadline	03.12.2026 - 12.00 (Brussels time)
Directorate-General (full name)	Directorate-General for Climate Action
Unit	CLIMA.E.TRO – Taskforce for Resilient Operations
Place of assignment	Brussels
Grade range	AD5-11
Domain	CLIMATE
Contract type	Temporary Agent 2a

About us ("We are")

The European Commission is organising an external selection procedure for a temporary agent to fill the post of Team Leader – Principal Operations Officer. The officer will be a part of the taskforce whose main goal is to prepare establishment of a dedicated "secure ETS operations office" by 2028, where all reviewed processes and streamlined administrative tasks will benefit from efficiency gains and financial sector grade information security services. This taskforce will be hosted by the Directorate-General for Climate Action (DG CLIMA) and report directly to the Director for Climate Resilience and Information Management of DG CLIMA.

The taskforce is established with the aim to retain operational excellence and continuity of the ETS (Emissions Trading System) Registry in an evolving and increasingly challenging geopolitical and cybersecurity landscape. The taskforce will enhance the current operating model, by aspiring to ensure maximum compliance with applicable regulations for comparable financial market infrastructures and to minimise exposure of the critical climate information systems to external threats thereby contributing to predictable and stable policies and business continuity.

ETS operations are centralised in a single information system, called the Union Registry. It holds carbon emission allowances in accounts for more than 15,000 operators from the power sector and energy intensive industry, including the aviation sector. Emission allowances are considered financial instruments under MiFID, and the registry offers services similar to the notary and central maintenance services offered by Central Securities Depositories ('CSD').

About the role ("We propose")

The Operations management function will form an integral part of the first line (of defence), and its mission is to support ETS Office in achieving its goals and delivering its strategy through providing robust, compliant and resilient operational activities. We offer an exceptional opportunity to help establish a modern enterprise operational architecture from the ground up. As a key member of the initial team establishing the future ETS Office in Brussels, you will co-create, design, implement and later enhance the office's operational resilience framework. The role ensures that critical services, processes and supporting capabilities remain resilient under disruption and that the institution is well positioned to prevent, respond to, recover from and learn from operational incidents, in line with regulatory expectations and business needs.

The Principal Operations Officer will contribute to the design, implementation and maturation of the institution's operational resilience framework, with particular focus on critical functions, severe but plausible scenarios, incident management, business continuity, disaster recovery, third-party dependencies and ICT-related resilience under DORA and related standards. Working across business, operations, technology, risk, compliance and senior governance bodies, you will support a coherent end-to-end approach to resilience in an environment where continuity, market confidence and systemic stability are essential.

In close coordination with the relevant management, legal, risk, internal audit and compliance functions, the Principal Operations Officer will oversee all components of the institution's operational resilience, business continuity and crisis management framework. The role equally offers the opportunity to:

- lead the first line of defence of the risk management strategy of the Office;
- lead the internal team of experts and manage services in outsourced contracts to strengthen the institution's preparedness for ICT disruptions, cyber incidents, outsourcing failures and cross-functional crisis events;
- work with first and second line functions to strengthen incident management, crisis preparedness, business continuity and disaster recovery capabilities;
- identify and map important business services, critical processes, dependencies and vulnerabilities;
- engage with internal and external stakeholders, including control functions, senior committees, critical providers and supervisory authorities, to support in the definition and monitoring of impact tolerances, resilience indicators and associated governance arrangements;
- assess resilience risks related to people, processes, technology, facilities, cyber threats, data and third-party dependencies, promoting resilience awareness and cross-functional collaboration throughout the organisation.

Qualifications, experience and skills ("We look for")

We are looking for a Team Leader - Principal Operations Officer.

A post-aligned academic qualification is preferred, such as master's degree in business administration, telecommunications, information systems, finance, economics or highly relevant engineering field. Familiarity with the regulatory environment affecting financial institutions, especially in relation to operational and digital resilience would be a strong asset.

Additionally, the ideal candidate should have:

- a minimum of 12 years of relevant professional experience in a public or private sector (preferably finance) institution;

- experience in operational resilience, operational risk, business continuity, ICT risk, cyber resilience or a closely related area;

- demonstrated experience in developing and implementing operational resilience frameworks, including service mapping, impact tolerances or equivalent continuity metrics, dependency analysis, scenario testing and crisis coordination;

- strong understanding of the EU regulatory framework relevant to resilience and ICT risk, notably Digital Operational Resilience Act (DORA), and familiarity with related expectations under European Market Infrastructure Regulation (EMIR), Central Securities Depositories Regulation (CSDR), Markets in Financial Instruments Directive/Regulation (MiFID/MiFIR)-related interfaces, Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), in particular with relation to outsourcing and cybersecurity requirements;

- experience in cross-functional coordination involving operations, technology, risk, security and governance stakeholders;

- an understanding of post-trading activities, settlement cycles, asset servicing, collateral processes, reconciliations and control frameworks is desirable;

- familiarity with the regulatory and operational environment applicable to financial market infrastructures, custodians, payment systems or major financial institutions would be highly desirable;

- relevant information systems, cybersecurity, business continuity and service management certifications such as MBCI, CBCI, CRISC, CISM, CISSP, ISO27001, ISO22301, ITIL and equivalent would be strong assets;

- proven experience with threat-led testing, incident response, disaster recovery, third-party risk, cloud dependency management and cyber resilience exercises organised by central institutions are significant assets.

Other valued qualities: Strong analytical, organisational and problem-solving skills with the ability to work across functions and coordinate with business, technology and control stakeholders. The ability to lead and manage teams (internal and outsourced) and engage with business managers, regulators, auditors and other control functions is also crucial.

Familiarity with the European Commission environment, including security practices, methodologies and roles (ITSRM, LSO / LISO, CRO, GRC, etc.), will be valued but is not indispensable.

Given the nature of the role, the selected individual will embark on the EU security clearance process. Fluency in English, both spoken and written, is indispensable.

The recruitment grade will be determined in accordance with Article 13 of Commission Decision C(2025)4716, taking account of the candidate's recognised professional experience. In exceptional and duly justified cases, the Authority Authorised to Conclude Employment contracts (AACE) may authorise classification in higher grade with fewer years of professional experience than normally required under that Article.

How to express your interest?

You should send your documents in a single pdf in the following order:

1. your CV 2. completed application form.

Please send these documents by the publication deadline to CLIMA-E-ARES@ec.europa.eu, Elina.BARDRAM@ec.europa.eu and Javier.CACERES@ec.europa.euindicating the selection reference CLIMA/COM/2026/526348 in the subject.

No applications will be accepted after the publication deadline.

Eligibility

For eligibility please consult this page with all the information needed.